

UNITED STATES DISTRICT COURT

FILED

NORTHERN

DISTRICT OF

ILLINOIS, EASTERN DIVISION

UNITED STATES OF AMERICA

v.

HANJUAN JIN

MICHAEL W. DOBBINS
CLERK, U.S. DISTRICT COURT

CRIMINAL COMPLAINT
CASE NUMBER
08CR0192
UNDER SEAL

MAGISTRATE JUDGE BROWN


I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. From on or about February 23 to February 28, 2007, in Cook County, in the Northern District of Illinois defendant did,

knowingly steal, or without authorization appropriate, take, carry away or conceal a trade secret that is related to or included in a product that is produced or placed in interstate or foreign commerce, for the economic benefit of anyone other than the owner of the trade secret, intending or knowing that the offense will injure any owner of that trade secret,

in violation of Title 18 United States Code, Section 1832.

I further state that I am a(n) Special Agent with the Federal Bureau of Investigation and that this complaint is based on the following facts: See Attached Affidavit

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

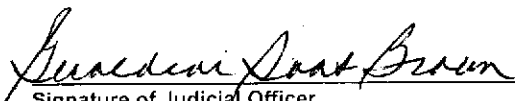

Signature of Complainant

Sworn to before me and subscribed in my presence,

March 3, 2008
Date

at Chicago, Illinois
City and State

MAGISTRATE JUDGE
GERALDINE SOAT BROWN
Geraldine Soat Brown
U.S. MAGISTRATE JUDGE


Signature of Judicial Officer

FILED
March 03, 2008
MAR 03 2008

MICHAEL W. DOBBINS
CLERK, U.S. DISTRICT COURT

STATE OF ILLINOIS)
)
COUNTY OF COOK)

AFFIDAVIT

I, Michael R. Diekmann, being duly sworn, depose and state as follows:

I. PRELIMINARY INFORMATION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and I have been employed by the FBI for over four years. I am currently assigned to the Chicago Division. In my capacity as a Special Agent, I have received specialized training and have investigated violations of Federal criminal laws and regulations, including offenses relating to economic espionage and theft of trade secrets, in violation of Title 18, United States Code, Sections 1831 and 1832.

2. The information provided below is for the limited purpose of establishing probable cause to believe that HANJUAN JIN ("JIN") did knowingly steal, or without authorization appropriate, take, carry away or conceal a trade secret that is related to or included in a product that is produced or placed in interstate or foreign commerce, for the economic benefit of anyone other than the owner of the trade secret, intending or knowing that the offense will injure any owner of that trade secret in violation of Title 18, United States Code, Section 1832.

3. This affidavit is based upon my personal observations, interviews of witnesses, review of documents, reports, as well as information received from other law enforcement agents and investigators. Because of the limited purpose of this affidavit, it does not contain all information that is known to law enforcement regarding this investigation.

II. JIN WAS STOPPED AT THE AIRPORT AND INTERVIEWED ON FEBRUARY 28, 2007, MARCH 1, 2007 AND MARCH 2, 2007.

4. On February 28, 2007, JIN was stopped by officers employed by the United States Customs and Border Protection ("CBP") during a random outbound search at O'Hare International Airport in Chicago, Illinois. At the time, JIN was traveling on a one-way ticket to Beijing, China. During the stop, officers from CBP asked JIN if she had any currency to declare. JIN stated that she had \$10,000 in United States currency in her carry-on luggage.

5. The officers searched JIN's carry-on and discovered approximately \$30,000.00 in United States currency in her possession. JIN's incorrect declaration of the United States currency led CBP to further inspect JIN's carry-on luggage. This further inspection revealed several technical documents labeled "[Company A] Confidential Proprietary," approximately seven documents written in Chinese ("Chinese Hard Copy Documents"), a European company's product catalog of military technology written in English ("Catalog"), and a technical manual written in Chinese ("Manual"). Also in JIN's possession at the time of the search were a personal computer laptop, a thumb drive, four external hard drives, 29 recordable compact discs, and one videotape.

6. Shortly thereafter, JIN gave verbal consent for the CBP agents interviewing her to review her laptop computer. JIN typed in her username and password. A subsequent search of JIN's laptop computer revealed numerous Company A documents noted on their face as "[Company A] Confidential Proprietary." The thumb drive and external hard drives were also reviewed and found to contain Company A documents, which were also marked on their face as "[Company A] Confidential Proprietary." Around this time, JIN informed CBP agents that JIN worked for Company A.

7. Around this same time, JIN waived her Miranda rights and she agreed to speak with

law enforcement. During this interview, JIN stated that she had been on medical leave from Company A since May 2006. JIN further stated that because she had been off from work for such a long time, she wanted to use the Company A documents to refresh her knowledge.

8. During the same interview, JIN was shown a Company A document, found in JIN's bag at the airport by CBP, entitled "Protection of Proprietary Information," which describes Company A's policies regarding the treatment of proprietary information. For instance, this document states that Company A employees are responsible for proprietary information and legal recourse will result from unauthorized disclosures. The document has handwritten notes on it. JIN stated that the handwriting found on the document was hers, but claimed to have never read the document.

9. JIN also stated that she worked on software for Company A, while also working on software for Company B on a full time basis. Company B is based in the Chicago suburbs, as is Company A. JIN stated that she was hired by Company B in March 2005. JIN stated she never informed anyone at Company A that she was employed at Company B, and that one of her former supervisors for Company A (Individual 1) was now one of the owners of Company B. According to Company A representatives, Company B is a competitor of Company A in the telecommunications industry.

10. During the same interview, JIN stated that Individual 2 gave her the Catalog. She later stated during this same interview that Individual 2 works for Company C, which is based in China. JIN described Individual 2 as an engineer with expertise in computer software. JIN stated that Individual 2 provided her the Catalog to look over, but with no specific instructions. JIN said she did not know how Individual 2 obtained the Catalog.

11. JIN also stated that Individual 2 has a business relationship with Individual 1, through Company B. JIN stated that she does not know the name of Individual 2's company but that it purchased equipment from Company B. JIN stated she does not believe that Individual 2 works for the Chinese government or military.

12. At the conclusion of the interview on February 28, 2007, JIN left the airport and returned to her home in the Northern District of Illinois. The CBP agents retained possession of the various Company A documents because they were technical documents, marked as confidential proprietary and JIN stated that she was not actively employed with Company A.

13. JIN was stopped again on March 1, 2007 at the airport in Chicago, when she was again trying to depart on a one-way ticket to Beijing, China. At this time, she waived her Miranda rights and agreed to speak with law enforcement agents. During the subsequent interview, which was conducted by agents of the FBI, JIN was asked about the documents marked as proprietary that previously had been seized from her at the airport, and JIN stated that she was taking these documents with her to China to refresh her memory on the material and prepare herself for her next job.

14. Later, after the interview, JIN consented to a search of her residence. During the search, agents of the FBI discovered multiple binders of documents marked as containing confidential and proprietary information belonging to Company A. The various Company A documents were seized from JIN because they were technical documents, marked as confidential proprietary and agents had confirmed with Company A that JIN no longer worked for Company A. For similar reasons, agents also seized the Company A laptop computer that was issued to JIN in connection with her employment and found inside her residence.

15. JIN was interviewed at her residence on March 2, 2007. After again waiving her Miranda rights, JIN stated that Individual 1 introduced her to Individual 2 at the end of April 2005 in Beijing, China. JIN stated that at the time of this introduction she was working for Company A and Company B. At this initial meeting, Individual 1 introduced Individual 2 to JIN as one of Individual 1's friends. During the meeting, JIN informed Individual 2 that she was working for a telecommunications company.

16. JIN also stated that she met with Individual 2 a second time in November 2005 in Beijing, China. JIN stated that this meeting was attended by her and Individual 2 alone. At this meeting, Individual 2 provided JIN with his phone number. According to JIN, Individual 2 also instructed her (JIN) to use the phone number when she was in Beijing in order for them to arrange meetings. JIN stated that this second meeting was more like an interview with Individual 2.

17. JIN also stated that between November 2006 and February 2007, a third meeting between JIN and Individual 2 took place in Beijing, China. At this third meeting, JIN stated that Individual 2 wanted to determine whether JIN could contribute to the "Short Message" project. At this time, JIN was provided with the Chinese Hard Copy Documents by Individual 2 at a restaurant. The Chinese Hard Copy Documents generally reference Chinese military telecommunications systems. One of the documents was entitled "Data Packet Format Protocol of Artillery's Quick Counter Short Messaging Application System." JIN also stated that Individual 2 requested JIN to review the documents in order to determine the amount of assistance JIN would be able to provide on the project. According to JIN, Individual 2 did not offer to pay her for this assistance and did not provide any instructions to her on how to handle these documents, despite the fact that some of them were marked as classified Chinese documents.

18. JIN stated that she understood Individual 2's request at the third meeting to be an opportunity to prove herself and obtain employment. JIN stated that she told Individual 2 that she agreed to help and would provide information to him. JIN indicated that she believed her assistance associated with this project might result in a job for her at Company C. JIN stated that Individual 2 did not give her very much information about Company C. However, JIN stated that she had visited Individual 2's office at Company C, which is located in Beijing.

19. JIN also stated that she planned to meet with Individual 2 in Beijing, during her trip to China, originally scheduled for February 28, 2007. JIN believed that on this return trip she would have been offered employment at Company C.

III. COMPANY A DOCUMENTS IN JIN'S POSSESSION ON FEBRUARY 28, 2007

20. During the investigation, law enforcement met with representatives of Company A regarding the various documents that were found in JIN's possession at the airport on February 28, 2007. Company A representatives identified many of these documents as trade secrets related to Company A's business. For instance, according to a Company A systems engineer ("Systems Engineer"), one of these documents ("Document 1") provides a detailed description on how Company A provides a specific interstate communication feature that Company A incorporates into its telecommunication products, which are distributed by Company A to customers throughout the United States and elsewhere. Document 1 includes the necessary architecture for the feature and explains how to expand the network for the feature. Company A's Systems Engineer further stated that currently, Document 1 relates to technology in which Company A has invested large amount of money on research and development. According to Systems Engineer, this technology is one of the largest and most profitable areas of Company A's business. Systems Engineer further stated that

if another company was to receive information on this technology and was able to replicate it, Company A would sustain substantial economic harm. Document 1 was found on an external hard drive seized from JIN at the airport on February 28, 2007. Systems Engineer also stated that JIN's work assignments within Company A did not require her access to Document 1.

21. Document 1 was marked "[Company A] Confidential Proprietary" and was maintained on Company A's secured computer network. Company A employees must log on to this secured network to get access to Document 1 and other Company A documents. Company A also has physical security measures in place, such as posted security guards, identification card access for employees, and security cameras. Company A also has employees sign agreements in which they agree not to disclose confidential information of Company A to others. According to Company A representatives, Document 1 was never shared with customers or outside Company A and is completely an internal document. The document was created to teach teams within Company A how to create this specific feature.

22. Company A representatives also estimated the negative financial ramifications that would result from certain documents taken by JIN being made public. More specifically, Company A representatives from Company A's legal, security and engineering departments, reviewed six documents, including Document 1, to assess the damage to Company A if these documents became available to its competitors. Each of these documents was found on an external hard drive seized from JIN on February 28, 2007. Each document references and discusses the same proprietary technology described in Document 1. Also, Company A representatives, including Systems Engineer and an engineer operations manger ("Engineer Operations Manager"), stated that the documents were trade secrets. The same security measures are in place to protect these additional

documents as previously described as to Document 1. Company A representatives, including Engineer Operations Manager and a representative from Company A's legal department, estimated that if these six proprietary documents became public, Company A could lose substantial global revenues over the next three years, and that the research and development costs for the proprietary information in JIN's possession exceeded \$600 million.

23. In addition, a search of the computer and hard drives seized from JIN at the airport on February 28, 2007 revealed that JIN was in possession of approximately 1300 source code files. A representative of Company A that works in wireless security services identified these source code files as belonging to Company A, and stated that Company A employees should never have the need to store source code on a laptop computer. According to Systems Engineer, all of Company A's source code is labeled and/or marked as Confidential Proprietary.

IV. JIN'S ACTIVITIES WHILE ON SICK LEAVE FROM COMPANY A

24. Shortly after JIN was stopped by CBP at the airport, law enforcement agents interviewed representatives of Company A regarding JIN's employments and obtained documents regarding JIN's employment at Company A.

25. According to Engineer Operations Manager, JIN started working for Company A in approximately 1998 as a software engineer. JIN signed an employment agreement around this time, stating that she would not disclose confidential information of Company A, except as her duties may require.

26. Company A records show that while employed by Company A, JIN took two leaves of absence. The first was from approximately June 2005 to September 2005. JIN took a second leave of absence from Company A from approximately February 2006 to February 2007. Both of

these leave requests were for medical reasons. According to Company A records, JIN was only approved for disability by Company A from February 15, 2006 to October 9, 2006, during her second leave of absence.

27. According to Company A documents, on or about October 27, 2006, JIN provided Company A with a certification from a doctor that she was too ill to return to work. This doctor's note stated that JIN was to receive 9 to 12 additional months of treatment.

28. According to Company A records, JIN continued to access Company A documents during her two sick leaves. Company A records show that during her first sick leave, JIN accessed Company A documents from the Company A's internal document sharing system (Network A). In addition, Company A records show that during her second leave of absence, JIN continued to access Company A's network and download proprietary documents.

29. According to Company A documents that summarize its computer network logs, from approximately August 2006 until November 2006, during JIN's second leave of absence from Company A, JIN accessed Company A's network from inside Company B's offices. More specifically, a summary of Company A's network logs shows that Company A's network was accessed by JIN using an IP address which is used by Company B. This IP address was verified on the American Registry of Internet Numbers as belonging to Company B.

30. According to a representative of Company A that works in wireless security services, in order for JIN to access Company A's network from a computer outside Company A, JIN would have to install Company A's custom access software on that outside computer.

31. According to JIN's airline records, JIN returned to Chicago from a trip to China on February 15, 2007. According to Company A records, JIN logged onto Company A's network

while she was in China on multiple occasions on February 6, 8, 9, and 13, 2007.

32. According to Company A documents, on February 18, 2007, while still on sick leave from Company A, JIN accessed numerous Company A computer files starting at approximately 1:53 p.m., and downloaded seven Company A documents. According to Company A representatives, these documents contain information pertaining to Company A's proprietary technology.

33. Also, on February 19, 2007, JIN again accessed numerous Company A computer files starting at approximately 7:56 p.m., and downloaded thirteen Company A documents. These documents included information about Company A's technology. These documents also included subject matters that JIN had not been assigned to during her employment with Company A.

34. According to bank records, on February 21, 2007, \$10,000 was withdrawn from a bank account held by JIN and her husband.

35. According to JIN's airline records, on February 23, 2007, JIN purchased a one-way ticket to China for a flight that was scheduled to leave on February 28, 2007 at approximately 12:22 p.m.

V. JIN'S ACTIVITIES AFTER RETURNING TO COMPANY A FROM SICK LEAVE

36. According to a nurse's log at Company A, JIN returned to Company A on February 21, 2007 and asked security personnel for a nurse who could clear JIN to return to work. According to these same nurse's log, JIN was later informed by a nurse with Company A that she needed a return-to-work document certified by her doctor. This nurse also told JIN to bring the form back to Company A on February 26, 2007.

37. On February 23, 2007, JIN returned to Company A with the return-to-work document signed by her doctor, stating that she was cleared for full time work and had no medical

restrictions. As a result, on the same day, JIN's security badge with Company A was re-activated and her manager ("JIN's Manager"), was notified of her return to work.

38. According to Company A records, JIN later arrived at Company A on February 26, 2007 at approximately 9:00 a.m. This same day, JIN's Manager stated that he met with JIN in JIN's Manager's office at Company A to discuss JIN's return to work. According to JIN's Manager, JIN informed JIN's Manager during this meeting that she wanted to return to work full time, and expressed an interest in future Company A projects. According to JIN's Manager, this was the first time JIN's Manager and JIN had met. JIN's Manager stated that he had become JIN's supervisor while JIN was out on sick leave. JIN's Manager stated that he did not assign JIN any assignments or work of any kind during this meeting. During this meeting, JIN's Manager stated that JIN informed JIN's Manager that she had no medical restrictions on her future work with Company A.

39. According to Company A records, which reflect the dates and times that employees enter and leave Company A buildings, JIN left her assigned Company A building on February 26, 2007 at approximately 4:30 pm. Company A records show that JIN accessed numerous Company A computer files starting at 9:51 a.m. and ending at 10:35 p.m. that same day. According to Company A records, JIN downloaded approximately 232 documents from Company A's internal network during this time period, with her activity nearly continuous from 9:51 a.m. until 2:23 p.m. At this time, JIN had no work assignments with Company A, let alone assignments that would have required her access to these computer files.

40. According to a Company A representative, who reviewed the documents accessed by JIN on February 26, 2007 at the request of law enforcement, many of the accessed documents were outside the scope of JIN's prior work with Company A.

41. Company A surveillance tapes show that JIN returned to her assigned Company A building at approximately 8:50 p.m. on February 26, 2007. She was recorded entering a door in the building where she works after passing through a security gate. At approximately 12:17 a.m. on February 27, 2007, Company A surveillance tapes show that JIN exited the after hours door of the same building with two large bags that appeared to be full. These surveillance tapes also show that JIN return approximately one minute later. At approximately 12:23 a.m. that same morning, JIN left the same Company A building with what appeared to be a 3-ring binder, numerous paper documents, and multiple books.

42. According to Company A records, on February 27, 2007, JIN emailed JIN's Manager at approximately 12:13 p.m. In this email, JIN stated that she was not ready to return to work due to her illness. She stated that she was willing to "volunteer the laying off now".

43. Later that same day, JIN's Manager responded to JIN's email, stating that he wanted to speak with JIN about JIN's request and her email. According to JIN's Manager, JIN did not respond to JIN's Manager's email.

44. However, according to Company A records, later on February 27, 2007, JIN logged onto Company A's network and downloaded approximately 65 documents.

45. Moreover, Company A surveillance tapes show that JIN returned to Company A on February 27, 2007, at approximately 10:19 p.m. According to Company A records, JIN began accessing Company A documents from their network at approximately 10:49 p.m., with the last document accessed at approximately 1:34 a.m on February 28, 2007. These documents included documents related to the telecommunications networks used by public safety organizations in Europe, the Middle East, and Africa as well as Company A's products for those networks. JIN was

then recorded on Company A surveillance tapes leaving Company A at approximately 12:46 a.m. on February 28, 2007 with her Company A laptop.

46. According to bank records, on February 27, 2007, a withdrawal of \$20,000 was made from JIN and her husband's bank account at approximately 3:06 p.m., after she had sent her email to JIN's Manager at Company A. Bank records also show that on or about March 5, 2007, \$115,000.00 was transferred from this same account to a bank account at China Merchants Bank in Lanzhou, China.

VI. JIN'S WORK FOR COMPANY B

47. According to emails found on JIN's computers, JIN was consulting on projects for Company B as early as September 2004.

48. According to JIN's bank records, JIN received a salary from Company B from approximately April 2005 to November 2006.

49. According to Company A representatives, Company B is a competitor of Company A in the telecommunications industry and has previously hired a number of former Company A employees.

50. According to Company B's website, Individual 1 is the Chief Technology Officer for Company B. Representatives of Company A confirmed that Individual 1 was a former employee of Company A.

VII. JIN'S EMAILS DEMONSTRATING HER INTENT TO RETURN TO CHINA TO WORK FOR COMPANY C.

51. Law enforcement obtained emails from JIN's personal laptop seized at the airport on February 28, 2007, written in Chinese, between JIN and Individual 3, who works for Company C. On or about June 23, 2006, JIN sent Individual 3 an email saying that she had hoped to return to

China by the end of June of 2006, but her poor health situation prevented her from doing so. JIN stated in the email that she would return to China as soon as her health situation was under control. She provided that her possible return date to China would be around the end of August. On June 23, 2006, JIN wrote "I hope I am not causing you troubles in arranging the work. Please send me some document related to the project, if possible, so that I could prepare something at home."

52. Individual 3 responded to JIN one week later and wrote "It is entirely up to you to determine the date of your return. Of course, I would like you to join our team as soon as possible. I will mail you the file that contains the document related to our project." Individual 3 then stated "Do you want me to prepare something before your return, such as your residence, etc.?"

53. JIN responded to Individual 3 on September 6, 2006 stating that she would have to postpone her return date to China again. JIN told Individual 3 "I will join your team with high spirit and good physical condition." JIN stated further that she would like to purchase a residence in Beijing, but in the meantime she meant to rent a place close to Individual 3's company.

54. Approximately one week later on September 7, 2006 Individual 3 responded "Do not hesitate to let the company know your demands once you are back. I guess (we should) make sure your income level is not lower than that in the U.S. and on top of that you should be entitled to an appropriate percentage of dividend. You should share with us the fruit of our collective effort."

55. JIN later responded to Individual 3 stating "Thank you for each of your return emails, which make me really feel that I am going to be a member of your team soon. My return plan has a solid date at last (I feel very guilty that my return was postponed again and again for almost half a year)!". JIN further stated "Your considerations about the income are especially moving, fully demonstrating your sincerity and generosity. I am not putting forward a harsh-termed salary

demand. I fully trust that you will make a reasonable and attractive offer. I fully understand the differences between China and the U.S. and I will not compare it with the U.S. income. A proactive and relaxed working environment is more important to me. I will do my best to contribute to the continuous growth of the company." JIN then stated, " Next week, I am going to resign from [Company B] and make an airline reservation". JIN also stated "please issue me a formal letter of appointment, if possible, so that I have more comprehensive and detailed understanding of my job responsibilities."

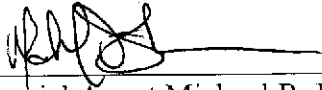
56. According to bank records, JIN stopped receiving a Company B salary on or about November 2006. Also, JIN's travel records show that JIN left for China on November 16, 2006.

57. Further searches on JIN's personal laptop showed that on January 28, 2007, JIN sent Individual 1 an email stating that she had no problems with her health and wanted to get back to working. JIN stated "After many comparisons and much pondering, I find that I like to work with [Individual 3] in [Company C]. I have some basic knowledge about their products and I feel pretty compatible with these people, although I met them briefly for only two times. I like a relaxed and familiar working environment and I hope that this choice of mine could win your support and assistance. Should [Individual 3] ever mention me, please put in some good words for me." Individual 1 responded to JIN's email on February 7, 2007, stating that he/she had tried to reach JIN by calling three of her telephone numbers. Individual 1 instructed JIN to call his/her mobile phone, and stated that he/she was currently in Shanghai.

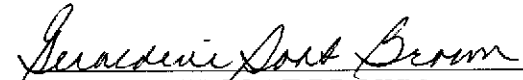
CONCLUSION

58. Based on the information above, there is probable cause to believe that HAN JUAN JIN ("JIN") did knowingly steal, or without authorization appropriate, take, carry away or conceal a trade secret that is related to or included in a product that is produced or placed in interstate or foreign commerce, for the economic benefit of anyone other than the owner of the trade secret, intending or knowing that the offense will injure any owner of that trade secret in violation of Title 18, United States Code, Section 1832.

FURTHER AFFIANT SAYETH NOT


Special Agent Michael R. Diekmann
Federal Bureau of Investigation

Sworn and subscribed to before me, this 3rd Day of March, 2008


GERALDINE GOAT BROWN
UNITED STATES MAGISTRATE JUDGE